*Güvenlik Bilimleri Dergisi / Journal of Security Sciences*

***Jandarma ve Sahil Güvenlik Akademisi***
***Güvenlik Bilimleri Enstitüsü***
***Güvenlik Bilimleri Dergisi, 2. Uluslararası Güvenlik Kongresi Özel Sayısı (İstihbarat ve Güvenlik), 157-174, doi:10.28956/gbd.1007953***

*Gendarmerie and Coast Guard Academy*
*Institute of Security Sciences*
*Journal of Security Sciences, The Special Issue of the 2nd International Security Congress (Intelligence & Security), 157-174, doi:10.28956/gbd.1007953*

**Makale Türü ve Başlığı / Article Type and Title**
Konferans Bildirisi / Conference Paper
Terörizmin Finansmanını Takip Programı Kapsamında Veri Paylaşımı: Swıft Ağı Güvenliği ve Kişisel Verilerin Kullanılması
Data Sharing Under Terrorist Finance Tracking Programme: Swift Network Security and Use of Personal Data

**Yazar(lar) / Writer(s)**
Utkuhan YILDIRIM, Yüksek Lisans Öğrencisi, Karabük Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bölge Çalışmaları Anabilim Dalı, e-posta: utkuhanyildirim@gmail.com, Orc-ID: 0000-0001-8454-7801

**Bilgilendirme / Acknowledgement:**
-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur
-Bu makalede araştırma ve yayın etiğine uyulmuştur.
-23-25 Eylül 2021 tarihlerinde Jandarma ve Sahil Güvenlik Akademisi'nde icra edilen 2. Uluslararası Güvenlik Kongresi'nde sunulan tebliğin genişletilmiş halidir.

Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received : 18.10.2021
Makale Kabul Tarihi / Accepted : 23.12.2021

**Atıf Bilgisi / Citation:**
*Yıldırım, U. (2021). Terörizmin Finansmanını Takip Programı Kapsamında Veri Paylaşımı: Swıft Ağı Güvenliği ve Kişisel Verilerin Kullanılması, Güvenlik Bilimleri Dergisi, 2. Uluslararası Güvenlik Kongresi Özel Sayısı (İstihbarat ve Güvenlik), ss157-174, doi:10.28956/gbd.1007953*

# TERÖRİZMİN FİNANSMANI TAKİP PROGRAMI KAPSAMINDA VERİ PAYLAŞIMI: SWIFT AĞI GÜVENLİĞİ VE KİŞİSEL VERİLERİN KULLANILMASI

**Öz**

*Dijitalleşme, teknolojik araçların bankacılık sektörünün vazgeçilmez parçası hâline gelmesini sağlarken, küreselleşmeyse uluslararası iş birliklerinin gelişmesini sağlamıştır. 1973'te, yani kuruluşu itibariyle birkaç bankanın kendi aralarında veri mesajlaşmasını sağlayan, şirket işlevli bir kooperatif olan SWIFT, günümüzde uluslararası para transferlerinin yapıtaşı hâline gelmiştir. 2021'de 10.000'den fazla kullanıcının günlük 42 milyondan fazla işleminin başarıyla yapılmasını sağlayan SWIFT ağı, büyük bir veri akışını yönetmektedir.*

*2006 yılında The New York Times'ın ortaya çıkardığı bilgilere göre SWIFT ağından ABD, 11 Eylül sonrası terörün finansmanı hususunda bir iz bulmak için Belçikalı şirketten mahkeme celpleri aracılığıyla veri talebinde bulunmuştur. Avrupa Birliği ise bu gelişmeyi terör finansmanına müdahale edilmesinin haricinde, kişisel verilerin gizliliğini tehlikeye atan bir durum olarak görmüş; ihlallerle ilgili endişelerini dile getirmiştir. 2010'da Terörizmin Finansmanı Takip Programı (TFTP), ABD ve AB arasında imzalanan antlaşmayla resmiyet kazanmış, veriler sadece terör finansmanıyla ilgili paylaşılmaya müsait hâle getirilmiştir. Çalışmada, TFTP kapsamında SWIFT verilerinin akışı incelenmiş, kişisel verilerin korunmasıyla ilgili endişeler aktarılmıştır. Ülkelerin çıkar odaklı davranması hâlinde TFTP kapsamında elde edilen SWIFT verilerinin istismar edilebileceği ihtimali araştırmanın esas konusudur. İstismar ihtimallerine karşı tekelleşmenin önüne geçilmesi, yasal temsilcilikler ve şeffaflık gibi çözüm önerileriyle çalışma sonlandırılmıştır. Nitel araştırma özelliği taşıyan çalışmaya, bahsi geçen şirket verileri, resmî devlet belgeleri, gazeteler, akademik yayınlar kaynaklık etmiştir.*

***Anahtar Sözcükler**: Terörizmin Finansmanı Takip Programı, Swift, Kişisel Verilerin Kullanılması, Veri Güvenliği, Avrupa Birliği, TFTP*

# DATA SHARING WITHIN THE SCOPE OF THE MONITORING TERRORIST FINANCE TRACKING PROGRAMME: SWIFT NETWORK SECURITY AND USE OF PERSONAL DATA

**Abstract**

*While digitalization has enabled technological tools to become an indispensable part of the banking sector, globalization has enabled the development of international cooperation. SWIFT, which was a cooperative with a corporate function that provided data messaging between several banks since its establishment in 1973, has become the building block of international money transfers today. The SWIFT network, which successfully processed more than 42 million daily transactions of more than 10,000 users in 2021, manages a large data flow.*

*According to the information revealed by The New York Times in 2006, upon the request of the USA, data was requested from the Belgian company through subpoenas to find a trace of the financing of terrorism after September 11. The European Union, on the other hand, saw this development as a situation that endangered the confidentiality of personal data, apart from intervening in terrorist financing, and expressed its concerns about violations. In 2010, the Terrorist Finance Tracking Programme (TFTP) became official with the agreement signed between the USA and the EU, and the data was made available for sharing only on terrorist financing. In the study, the flow of SWIFT data within the scope of TFTP was examined and concerns about the protection of personal data were conveyed. The main subject of the research is the possibility that the SWIFT data obtained within the scope of TFTP can be exploited if the countries act in an interest-oriented manner. The study was concluded with solutions such as preventing monopolization, legal representations, and transparency against the possibility of abuse. The aforementioned company data, official government documents, newspapers, and academic publications have been the source of this qualitative research study.*

***Keywords:** Terrorist Finance Tracking Programme, Swift, Use of Personal Data, Data Security, European Union, TFTP*

## GİRİŞ

Teknolojik gelişmelerle beraber neredeyse her sektörün bir ilerleme sürecine girdiği gibi bankacılık sektörü de aktif bir gelişme süreci yaşamıştır. Bu süreçte, küreselleşme ve teknolojinin günlük hayatın bir parçası olmasıyla birçok ulusal ve uluslararası finansal işlem çevrim içi olarak yürütülmeye başlanmıştır. Bankacılıkta dijitalleşmenin çeşitli avantajları olduğu için teknolojiyle bütünleşme hızla artış göstermektedir. Bu hızlı dönüşüm süreci, dijitalleşmeyi bir tercih olmaktan çıkararak, bir zorunluluk hâline getirmektedir. Dijitalleşmenin tercih edilmesinin sebepleri, verimliliği arttırması, rekabet avantajları, kârlılığı arttırması gibi birçok başlıkta anlatılabilir. ATM sistemlerinin gelişmesiyle personel ihtiyacının azalması, mobil bankacılık ile fiziki ortama ihtiyaç duymadan işlemlerin yapılması, ödeme araçlarından kredi kartlarının büyük kolaylıklar sunması, kripto paraların piyasada yer etmesi, ticaretin elektronik ortamda büyük bir pazar payının olmasından kaynaklı çevrimiçi bankacılık sistemlerinin tercih edilmesi gibi durumlardan dolayı bankacılık teknolojiyle tamamen iç içe girmiş hâlde bulunmaktadır (Bakirtaş ve Ustaömer, 2019:9,14). Bankacılık sektöründe dijitalleşmenin beraberinde getirdiği en büyük kaygı, dijitalleşen verilerin güvenliği konusundadır.

Günümüzde uluslararası ödemeler neredeyse tamamen dijital ortama kaymıştır. 1973'te kurulan SWIFT (Society for Worldwide Interbank Financial Telecommunications) yani Türkçe olarak "Dünya Bankalar Arası Finansal Telekomünikasyon Derneği"nin ödeme ağı, uluslararası ödeme veri akışını sağlayan sistemlerdendir. Teknolojik dünyada uluslararası para transferi dendiğinde akla ilk gelenlerden biri SWIFT ağıdır. SWIFT Belçika merkezli bir uluslararası finansal mesajlaşma sistemidir. Şirket güvenlik ve hız bakımından kendini kanıtlamış ve dünyaca kabul görmüştür. Finansal sistemler birçok kurum ve bireyin önemli bilgilerini depoladığı için güvenlik ve veri gizliliği en temel konuları oluşturmakta ve SWIFT ağı bu şartları genel olarak sağlamaktadır (Kuzu, 2003:67). Fakat terörle mücadele amacıyla SWIFT'in, ABD Hazine Bakanlığının talepleri doğrultusunda verilerini yetkililere teslim ettiği ortaya çıkmıştır. Bu veri güvenliği ihlalinden sonra AB endişelerini dile getirmiştir. AB ve ABD'nin taraf olduğu, Terörizmin Finansmanı Takip Programı (Terrorist Finance Tracking Programme-TFTP), terör finansmanıyla ilgili verilerin, talep eden tarafa teslim edilmesini yasal bir statüde ve gizli olmadan yapılabilir hâle getirmiştir (Gür, 2009:180). Bu çalışmada SWIFT ağının genel olarak güvenliği incelenmiş; ardından 2006 yılında ortaya çıkan veri paylaşımı krizi üzerinde durulmuştur. "SWIFT ağı üzerinden kişisel veriler, yerel

çıkarlar doğrultusunda istismar edilebilir mi?" çalışmanın araştırma sorusudur. Ayrıca çalışmada, AB ülkelerinin TFTP kapsamında veri gözetlenmesinde kişisel verilerin korunmasıyla ilgili endişeleri işlenmiş ve bu görüşe katılır bir üslup ile çalışmaya devam edilmiştir. ABD Ulusal Güvenlik Ajansı'nın (National Security Agency-NSA) terörizmin finansmanı dışında SWIFT verilerini elde ettiğine dair çeşitli bilgiler bulunmaktadır. Elde edilen bilginin yerel çıkarlar doğrultusunda kullanılmasını engelleyecek hiçbir mekanizma bulunmamaktadır. Bu noktada TFTP, AB ülkelerinin endişe ettiği üzere kişisel verilerin korunması bakımından güvenlik açıklarıyla dolu gözükmektedir. Bu durumun çözümü için bu çalışmada tekelleşmenin önüne geçilmesi, yasal temsilcilikler ve şeffaflık gibi konularda bazı çözüm önerileri getirilmiştir. TFTP kapsamında SWIFT verilerinin gözetlenmesi günümüzde hâlâ çözüme kavuşmamış bir sorundur. Konuyla muhatap devletlerin yaşadığı mevcut problemler için çözüm önerileri sunulması ve muhatap olacak devletlerin ise mevcut problemlerden haberdar olarak bir gelecek projeksiyonu oluşturulması için zemin hazırlanması çalışmanın gayesidir. SWIFT ağı üzerinden kişisel verilerin istismarının mümkün olabileceği ve elde edilen verilerin, veri elde eden ülkelerce kendi çıkarları doğrultusunda kullanabileceği ihtimali üzerine bir düşünce ortaya koyulmuştur. Çalışmanın kapsamı SWIFT ağının TFTP üzerinden istismar edilme ihtimallerinin ortaya koyulmasından ibarettir. Çalışma nitel bir araştırma özelliği taşırken tümevarımcı bir yaklaşımla olaylar incelemektedir. Çalışmaya bahsi geçen şirket verileri, yayınlanan devlet resmî belgeleri, ulusal-uluslararası gazeteler, akademik kitaplar ve makaleler kaynaklık etmiştir.

## 1.1. GENEL OLARAK SWIFT AĞI VE 2006 ABD HAZİNE BAKANLIĞI İLE VERİ PAYLAŞIMI KRİZİ

Günümüzde uluslararası ödemeler neredeyse tamamen dijital ortama kaymıştır. 1973'te kurulan SWIFT (Society for Worldwide Interbank Financial Telecommunications) yani Türkçe olarak "Dünya Bankalar Arası Finansal Telekomünikasyon Derneği"nin ödeme ağı, uluslararası ödeme veri akışını sağlayan sistemlerdendir. 2021 verilerine göre hâlka açık olmayan kendi internet bağlantıları aracılığıyla, 10.000'den fazla kullanıcının ödemelerini birbirlerine ileten bu ağda her gün 42 milyon civarı ödeme işlemi verisi işlenmektedir (SWIFT, 2021b). SWIFT ağı, uluslararası ödemelerinin verilerini kendi ara yüzü aracılığıyla, güvenli ve hızlı bir şekilde ulaştırmaya çalışmaktadır. Son yıllarda sistemlerinde blok zincir teknolojisini de kullanmaya başlayan SWIFT ağı bu sayede, ödeme ile ilgili talimatların neredeyse para akışıyla eş zamanlı çalışmasını sağlamaktadır. SWIFT

kâr amacı gütmeyen, müşterilere ait hesapların düzenlenmesiyle ilgilenmeyen, uluslararası ödemelerde bir standart oluşturup güvenli ve hızlı işlem yapılmasını sağlayan finansal bir kuruluştur. SWIFT yapılan işlemlerle ilgili finansal bir mesajlaşma sistemi olarak düşünülebilir. Yıllardır biriken tecrübeyle belirli standartlara oturtulan bu ağın, yaklaşık 24 milyon günlük işlem yapılan bir yer olmasının yanında, kapasitesine rakip olacak başka bir yapıda bulunmamaktadır. Bu sebeple SWIFT, uluslararası para işlemlerinde, resmî bir zorunluluk içermese de kullanıcıların işlemlerini yapabilmesi için neredeyse zorunlu hâle gelmiştir (Talay ve Bayram, 2020: 948-954).

O hâlde SWIFT finansal bir mesajlaşma ağıdır demek bu sistemi oldukça iyi tanımlamaktadır. Kurumlar arası bir postacı gibi mesajlaşma sistemi sağlayan SWIFT uluslararası para transferlerinin veri akışını sağlamaktadır. Fonlar veya herhangi bir para SWIFT'e uğramadan, sadece doğrudan bankalar arasında işlem görmektedir. SWIFT bu durumları mesajlaşma aracılığıyla taraflara bildirmektedir. Sistem bankalar arası talimat, teyit ve rapor işlemleri yaparken, doğrudan ilişkisi olmayan bankalara ise muhabir banka sağlamaktadır. SWIFT kendi bilgi notunda aktardığı üzere, yasadışı faaliyetlere alet olmama politikası gütmektedir. Kullanıcıların gönderdiği mesajları izleyip kontrol etmeyen SWIFT, işlemlerin meşruiyetinin ve sorumluluklarının da yetkili finansal kuruluşlarda olduğunu ifade etmektedir. SWIFT'in Belçika'daki ana merkezinin yanında ABD'de de bir operasyon merkezi bulunmaktadır (SWIFT, 2021). Anlaşılacağı üzere, SWIFT sadece verileri belirli yerlere gönderme işini yapan bir mesajlaşma sistemidir. Bu sistem para akış kanalı değil; veri akış kanalı niteliği taşımaktadır.

2006 yılında SWIFT ile ilgili büyük bir kriz meydana gelmiştir. The New York Times'ın haberinde aktardığı bilgilere göre 11 Eylül saldırısı sonrasında ABD Başkanı George Bush'un gizlice bir operasyon başlatarak, El- Kaide Örgütü'ne finansal destek sağladığı düşünülen banka hesaplarını incelemek amacıyla Belçikalı SWIFT şirketinden veri akışı sağladığı ortaya çıkmıştır. Terörist ağlarının tespiti amacıyla, kamuoyuna açık başvurarak belge talep etmek yerine direkt SWIFT şirketi üzerinden bilgi almayı tercih eden ABD yönetimi, bu hamlesiyle birçok tartışmaya da zemin hazırlamıştır. Bazı uzmanların görüşlerine göre bu durum, verilerin gizliliği bağlamında büyük bir tahribat oluşturma potansiyeli taşımaktadır. Fakat ABD Hazine Bakanlığı, veri güvenliği bakımından bir problem olmadığı, sadece terör ile ilgili konularda veri akışı sağladıklarını hatta bağımsız bir denetim firması tarafından da bu durumun denetlendiğini aktarmıştır. Bu bilgilere alıkoyma işlemi

hakkında SWIFT şirketinden yapılan açıklamada, sadece terörün finansmanı ile alakalı durumlarda bu işlem yapılırken, uyuşturucu kaçakçılığı, vergi kaçakçılığı ve diğer terör dışı konularda veri paylaşılmadığı aktarılmıştır. SWIFT, ABD merkezli bir şirket olmamasına rağmen ABD'de de bir merkezi bulunmasından dolayı, Amerika Birleşik Devletleri'nin yasalarına tabi olmaktadır. Bu yasalar gereğince ortaya çıkan bazı imtiyazlar doğrultusunda SWIFT verilerine ulaşılmaktadır. Birçok uzman, bu durumda ABD vatandaşlarının kendi verilerinin de takip altında olduğunu düşündüğünü aktarmaktadır. Bu veri izleme işleminin, kişisel verileri korumaya yönelik endişeler duyulmasına sebep olduğu görülmüştür. ABD hükümeti geçmiş yıllarda henüz FTFP süreci The New York Times tarafından ifşa edilemeden bu konuyla ilgili resmileştirme çalışmaları yaparak, bu işlemi tamamen yasal ve halka açık bir hâle getirmeye çalıştıklarının sinyalini vermiştir (Lichtblau ve Risen, 2006). Yaşanan bu gelişme sonrası süreç hızlanmış ve bu yetkinin resmi olarak kullanılması konusunda adımlar atılmıştır.

2006'da yaşanan ABD Hazine Bakanlığına SWIFT ağının veri sağlaması olayıyla ilgili, mahremiyet ve veri korumayla ilgilenen Bağımsız 29. Madde Çalışma Grubu bir görüş bildirmiştir. 2007'de yayınlanan Avrupa Konseyi raporunda SWIFT verilerinin paylaşılma işleminin gerekli önlemler alınmadan, verilerin tam korunması sağlanmadan ve veri sahipleri bilgilendirilmeden yapılmaması gerektiği açıklanmıştır. SWIFT veri işleme ve paylaşma ile ilgili bu faaliyetlerin, 95/46 /EC sayılı direktifi uygulayan Belçika Veri Koruma Yasası'nı ihlal ettiği açıkça belirtilmiştir. Terörle mücadele adına bu verilerin sayesinde ciddi ilerleme sağladığını söyleyen ABD için özel bazı düzenlemeler ortaya koyulmuştur (Council of Europen Union, 2007). Yaşanan bu krizin ardından SWIFT ABD şubesi, şirketin ABD ile verilerini yasal zeminde paylaşmasına olanak sağlayacak olan Safe Harbor Prensipleri'ni kabul etmiştir. SWIFT' in ana merkezi Belçika'da olmasına rağmen ABD'nin iç finansal düzenlemelerine müdahâlede kullandığı bu prensiplere sıcak bakması, SWIFT'in durumu çözmeye yönelik şaşırtıcı bir adımı olarak görülmüştür (Gür, 2009:181). ABD, Safe Harbor doğrultusunda, terörle mücadele kapsamının dışında kalacak hiçbir veriyle ilgilenmeyeceğini taahhüt etmiştir. Ayrıca ABD Hazine Bakanlığı eline geçen verileri belirli periyotlarda silme taahhüdünü de vermiştir (Council of Europen Union, 2007).

Bunların var olmasının yanında, uluslararası bankacılık sistemleri içerisinde, her ne olursa olsun kurduğu sistemler sayesinde SWIFT'e güvenildiği bilinmektedir (Talay ve Bayram, 2020:948). Kullanıcı sayısı da bu düşünceyi kanıtlamaktadır. Şu

an bu kullanıcı sayısına yaklaşabilen bir başka alternatif ağ bulunmamaktadır. SWIFT ağı birçok uluslararası düzenlemeyi de dikkate almaktadır.

FATF (Financial Action Task Force-Mali Eylem Görev Gücü), OECD bünyesinde 1989 yılında G7 ülkelerinin kara para aklanmasının önüne geçmek adına kurduğu ve bu konuda belirli tavsiyeler ve standartlar üreten bir oluşumdur (Üstün, 2005:10). FATF, düzenleme, kontrol sağlama, uyum sağlama ve yaptırım uygulama gibi işlevlere sahiptir (Barbak, 2016:171). FATF tavsiyeleriyle kara paranın aklanması ve dolaylı yoldan terörizmin finansmanının kesilmesi adına kapsamlı çalışmalar yapılmıştır. Bu tavsiyelere göre AML/KYC gibi güvenliği teminat altına almaya çalışan çalışmalar mevcuttur. KYC (Know Your Customer) yani "Müşterini Tanı" ilkesi bu tavsiyeler içerisinde kilit bir noktadadır. İlk aşamada müşterinin kişisel kimlik ve adres verilerini doğruladıktan sonra bunları resmî belgeler üzerinden teyit ederek hareket eden KYC sistemi, sonrasında işlemi yapanın yetkili kişi olup olmadığını doğrulamaktadır. Sonrasında müşterinin uyruğu, eğitimi, bekleyen işlemleri, karşılıklı sık işlem yapılan hesapların tespiti gibi veriler elde edilmektedir. Bu sistem verileri, yüksek güvenlikli elektronik ortamda saklanmaktadır. Yetkili taraflar tarafından talep edilen belgelerin daha hızlı gönderilmesi, müşteriler hakkında istatistik ve risk haritaları oluşturulmasında bu sistemin varlığı oldukça önemlidir. Basel Bankacılık Denetim Komitesi ise bildirilerinde terör finansmanı ve kara para aklama üzerinde çalışmaların geliştirilmesini önermekte, "Müşterini Tanı" ilkesini risk değerlendirmesi açısından önemli bulmaktadır (Çakır, 2006: 44-45).

Güvenliği sağlamak adına ortaya koyulan müşteri tanılama sistemi birçok kişisel verinin saklanmasına sebep olmaktadır. Açıkça ifade edildiği üzere yetkililerce talep edilen belgeleri iletmek için ivedilikten de bahsedilmektedir. Kişisel verilerin gizliliği bakımından değerlendirildiğinde bu durumun yoruma açık kalmış bazı kısımları görülmektedir.

2001 ve 2003 yılında yayınlanan FATF tavsiyeleri açıkça terörizmin finansmanıyla mücadele ile alakalıdır. Kara para aklama ve bunun aracılığıyla terörizmi finanse etme ile ilgili FATF tavsiyeleri, bu konuyla alakalı BM sözleşmeleriyle ve diğer uluslararası sözleşmelerle eşgüdümlü hâle getirilmiştir (Üstün, 2005:11,14). Bu sözleşmelerde terör ve terör eylemleri açıkça belirtilmiştir. Uluslararası yapılarca terör faaliyeti olarak tanımlanan durumlarda müdahil olunabileceği anlaşılmıştır.

SWIFT'in 2006 yılında yaptığı açıklamalarda sadece terörle mücadele amacıyla bilgi paylaşımı yapıldığı aktarılmaktadır. Ancak SWIFT'in FATF kararlarını uygulayan bir şirket olduğu ve FATF'ın da asıl kuruluş amacının yasa dışı uyuşturucu faaliyetlerine müdahâle etmek olduğunu bilmek faydalı olacaktır (Yılmazcan, 1998:68). Böylece başlangıçta bile FATF kararlarını uygulayan bir yapının, terörle mücadele dışında da iş birlikleri yapmasına müsait bir hukuki zemin mevcuttur.

SWIFT'in kendi yayınlamış olduğu bilgilendirme kâğıdına göre şirket (Anti-Money Laundering and Counter-Terrorism Financing Rules (AML/CTF) düzenlemelerine tam uyumludur ve FATF kararlarını da bağlayıcı görmektedir ( SWIFT, 2016:2). AML/CTF Kara Para Aklama ve Terörizmin Finansmanını Önleme Standartlarını Değerlendirme Metodolojisi, 2004'te bu alanda çalışmaların yapılması için FATF tarafından yayınlanmıştır (Üstün, 2006:51). SWIFT ayrıca bu alandaki her kuruluş gibi ilk kez işlem yapan tarafın KYC kaydını yapabilmekte yetkilidir. Bugüne kadar 5.500'den fazla finans kurumu SWIFT'i tercih etmiştir (SWIFT, 2021a). FATF kararlarının bağlayıcı olmasından ve KYC ilkesinin zorunlu olmasından kaynaklı olarak, bu sektördeki her oluşum gibi SWIFT de yasal yollarla veri kaydı oluşturulabilir. Bu durum bankacılık sisteminin güvenliği için zaruri görülmektedir.

### 1.2. Terörizmin Finansmanı Takip Programı (TFTP) ve SWIFT

Terörizmin Finansmanı Takip Programı (Terrorist Finance Tracking Programme-TFTP) ABD yönetiminin başlattığı, terörün finansmanıyla mücadele etmek adına uluslararası finansal verilere erişmeyi yasal zemine taşıyan bir programdır. SWIFT'in kendi paylaştığı bilgi notunda, 2010'da ABD ve AB'nin imzalamış olduğu TFTP kapsamında yetkililerle iş birliği yapıldığı açıklamaktadır. ABD ve AB'den gelecek talepler SWIFT için bağlayıcı nitelik taşımaktadır. Bilgilerin sadece paylaşımıyla sorumlu olduğu durumlarda bu konulara şirket yorum getirmeyeceğini açıkça belirtmiştir (SWIFT, 2021a). Terörle mücadelede SWIFT devletlere olanak sağlama konusunda yardımcı olmaktadır.

SWIFT ağı dünya üzerinde en çok kullanılan finansal veri mesajlaşma sistemi olmasının yanında güvenilirlik bakımından da iyi bir imaj çizmiştir (Kuzu, 2003:67). Ancak uluslararası para transferi konusunda neredeyse tekel hâline gelen SWIFT, terörle mücadele kapsamında yapılan iş birliği çevresinde, şirket üzerinde nüfuzu olan ülkelerce istismar edilebilir bir yapı olmaya müsait hâle gelmiştir. Bunun sebebi

yetkililere bilgi akışını sağlayan düzenlemelerdir. Terörle mücadele edilmesi kapsamında bu yasanın kullanılması, terörün finansmanının kesilmesi ve dünyanın huzuru için oldukça işlevseldir. Ancak nüfuz sahibi ülkelerin istismarına da açıktır.

Küresel sistemde uluslararası çıkarların, ulusal çıkarlarla çatışması mümkündür. Teröre karşı yapılan iş birliklerinde dünya devletlerinin ortak bir görüşe sahip olmamasından kaynaklı olarak, aslında x ülkesinin terör örgütü olarak kabul etmemesine rağmen y ülkesinin terör örgütü olarak kabul ettiği bir örgüt var olabilmektedir. Ulusal bazda terör örgütü olarak kabul edilen yapılar, dünyada belirli güce sahip devletlerce terör örgütü olarak kabul edilmeyebilir. Terör örgütü olarak kabul etmeyen aynı zamanda SWIFT'in verilerine ulaşma yetkisi olan nüfuzlu x devletinin, para transferlerin takibini yasal olarak SWIFT veya başka bir şirket üzerinden elde etmesine rağmen duruma müdahâle etmemesi olası bir sonuçtur.

Ülkelerin bir yapıyı terör örgütü olarak kabul etme eylemi dışında, devletlerin terörle mücadele ettiği hukuki düzenlemeler de mevcuttur. Ancak devletlerin müdahâle edemediği, devletlerden fiili destekli, devlet himayeli, ya da devlet toleranslı terörizm faaliyetlerinin de olduğu bilinen bir gerçektir (Kedikli, 2013:132). İşte bu noktada fiili destekten daha az göze çarpacak olan, devletler tarafından terörün himaye edilmesi veya teröre tolerans sağlanması şeklinde ortaya çıkan uygulamalarda, finansal sistemlerle ilgili veri akışında, veriyi elde eden ülkenin, bunları kendi çıkarlarına göre kullanmasıdır.

Terörün tanımı noktasında bile fikir birliğine ulaşılamadığı düşünüldüğünde, ülkelerin hangi yapıları terör örgütü olarak kabul edip etmeyeceğinin ortak bir görüşte buluşması oldukça zordur. Terör örgütü olarak hangi yapıların kabul edilip edilmeyeceği devletlerin kendi iradelerinin altındadır. Bu noktada finansal piyasalarda istismara açık ve kişisel verilerin güvenliğini tehdit eden bu düzenleme açıkça bir revizyona ihtiyaç duymaktadır.

Terörün desteklenmesi veya göz yumulması gibi ihtimallerin dışında, diğer çıkarlar bakımından da elde edilen verilerin kullanılması ihtimali düşünülmelidir. Çıkarlar doğrultusunda veriler kullanılmasa bile, SWIFT üzerinde nüfuz sahibi ülkelerin, anlaşmazlık yaşadığı ülkelere yaptırım olarak sistemden çıkarma şeklinde tehdit ve cezalandırma uygulamaları gerçekleştirmesini sağlayabilir. Bu duruma en iyi örnek Rusya'nın SWIFT sisteminden çıkarılmayla tehdit edilmesidir (Rapoza, 2015). Bu tehdit sonucunda Rusya, 2018'de kendine muadil bir SWIFT sistemini kurmaya başlamış, 2019'da SPFS (System for Transfer of Financial Messages)

isimli sistem geliştirilip devreye sokmuştur. 2019'da yayımlanan habere göre SPFS'de 500 civarı katılımcı ile ülke içi para transferlerinin yüzde 18'i yapılmaktadır. Günümüzde sistem uluslararası kullanıma da açıktır (Rusya'nın "alternatif SWIFT" sistemi, 2019). Rusya, bu uygulamanın dışında küresel internet ağından da ayrılma projesini hayata geçirmiş, ulusal bir internet ağı kurulumunu tamamlamıştır. Kriz anlarında devreye sokulmak üzere planlanan bu proje, devletin ulusal verilerinin aslında çok büyük bir kısmının uluslararası düşmanlardan korunmasının da bir alt yapısıdır (Wakefield, 2019).

### *1.2.1. Öncül Suçlar, Kara Para Aklama ve Terör Finansmanı*

Öncül suçlar ve kara para aklama doğrudan veya dolaylı yoldan terörün finansmanıyla ilişkilendirilmeye müsait konulardır. Üstün'ün aktardığı üzere, AB Konseyinin önceki direktiflerinde, Viyana Sözleşmesi'nde belirtilen öncül suçlar, sadece uyuşturucu ile ilgili konuları öncül suç kapsamında değerlendirmekteyken, konseyin 2001/97/EEC sayılı direktifinde ve sonraki direktiflerde bu kapsam genişletilmiştir (2008:23-34). Ülkelerin mevzuatlarında belirtilmekte olan öncül suçların işlenmesiyle, elde edilen mali değer taşıyan, mal, evrak, taşınmaz gibi elde edilen çıkarlar da kara para olarak kabul edilmektedir (Şahin, 2010: 155,169).

Kara para aklamada öncül suçların kapsamının genişletilmesiyle birçok konuda veri akışı sağlanabilmektedir. SWIFT'in de konusu olan bu çalışmalar göz önüne alındığında 2006 yılında, "sadece terör ile ilgili konularda bilgi sağlanmaktadır" manasında verilen demeç, kara para aklamada öncül suç olma niteliğine yakınlık gösterebilecek bir para transferinin, terörün finansmanı kapsamında olmamasına rağmen öyleymişçesine değerlendirilebileceği ihtimalini düşündürmelidir. Bu noktada yasal şartlar sağlandığı için bilgi akışı da sağlanabilir. Şirket üzerinde nüfuzu olan ülkenin, kendi çıkarları doğrultusunda yasal zemini dayanak olarak alıp bu düzenlemeyi istismar etme ihtimali üzerine düşünülebilir.

Ortada bir kara para aklama olmamasına rağmen, ülke çıkarları doğrultusunda veri okumak isteyen ülke bu durumun şartlarını sağlayabilir. Kara para aklama üzerinden terörizm ile mücadele etmeye getirilen veri akışı, TFTP'nin kapsamında değerlendirilip SWIFT verileri gözetlenirse bu durumun istismar süreci başlamış olmaktadır. Bu ihtimaller de göz önünde bulundurularak, TFTP üzerinde yapılan herhangi bir iyileştirmede bu ve benzer kanallardan gelebilecek istismar ihtimalleri de değerlendirilmelidir.

### 1.3. TFTP Bağlamında Kişisel Verilerin Korunması Hakkındaki Endişeler

2006'da patlak veren SWIFT'in ABD ile veri paylaşımı krizi, Avrupa Parlamentosunun (AP) kişisel verileri koruma adına yaptığı çalışma ve düzenlemeleri tehdit etmiştir. Bu sebeple ilk aşamada bu durumun büyük veri ihlallerine sebep olduğu AP tarafından açıkça belirtilmiştir. Olayların ardından AP, kişisel verilerin korunması ve özel hayatın gizliliğini tahrip edecek bir ortam oluştuğunu ve Avrupa'da müttefiklerinin yürütmek istediği faaliyetlerden haberdar olmak istediğini aktarmıştır. Ayrıca TFTP'nin istismar edilerek, AB üye devletleri ve bireylerinin finansal işlemlerinde casusluk ihtimalinin olabileceğine dair endişe de göz önünde bulundurulmuştur. Sonrasında SWIFT'in Safe Harbor prensiplerine dâhil olması ile bu durum hukuki düzlemde kısmen çözüme ulaştırılmıştır. Belçika Mahremiyet Komisyonu da ABD ile yaşanan kriz sonrası düzenlemelerde, ABD'nin bilgi akışı ile ilgili şeffaflık ve sadece belirli alanlarla ilgileneceği, taahhütlerini tam manasıyla güvenilir bulmadığını ve bunun bir garantisi olmadığını ifade etmiştir (Gür, 2009:180-183). ABD ise ısrarla her yerden yaptığı açıklamalarda terörizm içerikli verilerle ilgilendiklerini söylemektedir. ABD Hazine Bakanlığının TFTP hakkında yayınladığı broşürde aktarıldığı üzere, SWIFT ağı üzerinden elde edilen veriler katı güvenlik düzenlemelerine tabidir. Bunun yanında yapılan veri talebi ile ilgili EUROPOL (European Police Office-Avrupa Polis Teşkilatı) bilgilendirilip, elde edilmek istenen verilerin birer kopyasının da buraya gönderileceği aktarılmaktadır (Terrorist Finance Tracking Programme, 2010). Avrupa polisi ile verilerin paylaşılması, şeffaflık adına önemli bir adım olarak kabul edilebilir. Fakat EUROPOL bir denetim mekanizması değildir. SWIFT, mesajlaşma ağı olduğu, bir banka veya ödeme sistemi formunda çalışmadığı için finansal denetim yapan denetçiler aracılığıyla denetlenememektedir (Gür, 2009:178).

Aslında veri güvenliği bakımından AP uzun yıllar çalışmalarını kararlılıkla sürdürmüş, bu konuda standartlaştırma adına önemli adımlar atmıştır. Ancak 2001 yılında yaşanan 11 Eylül saldırılarıyla beraber güvenlik önlemleri, mahremiyetin önüne geçmiştir. Bu noktada AP, TFTP gibi bazı konularda veri güvenliği açısından tavizler vermeye başlamıştır. SWIFT ağıyla ilgili kararlar bu durumun göstergesidir. AP bu durumu toparlamak adına birçok çalışma yürütmektedir. SWIFT işlemleri ile ilgili, Şubat 2010'da AB-ABD arasında yapılan görüşmede ortaya çıkan çalışma, veri koruma ile ilgili yetersizlikten kaynaklı reddedilmiştir. Temmuz 2010'da ise iyileştirmeler yapılarak bir SWIFT anlaşması kabul edilmiştir. İlkinden bariz farkı olmayan anlaşmanın, ikinci görüşmede kabul edilmesi, AP'nin ağırlığını, doğal

olarak da güvenliğe karşı kişisel verilerin ağırlığını, ortaya koymaya çalışması olarak yorumlanmıştır (Servent ve MacKenzie, 2011:391-393).

Avrupa Birliği birçok açıdan bu durumun ortaya çıkardığı endişeleri dile getirmiştir. TFTF'nin Avrupa'nın kendi veri koruma yasalarıyla uyumlu çalışıp çalışmayacağı ana endişe konusu olup, verilerin gizliliği korunmaya çalışılmaktadır. Bunların yanında SWIFT verileri, hesap numarası, kimlik numarası, işlem kaynağı ve alıcı gibi kişisel verileri içermekteyken ırksal, etnik, cinsel yönelim, siyasi veya dinî konular gibi hassas kişisel verileri barındırmamaktadır (Council of Europen Union, 2007).

2013'te ABD istihbarat devi NSA'nın (National Security Agency) küresel çapta bilgilere eriştiğine dair bir rapor, Brezilya'nın en büyük televizyon kanalı Globo tarafından yayınlanmıştır. Raporda, Google ve Brezilya'nın en büyük petrol firması Petrobras şirketinin ağları üzerinden ABD'ye veri aktırıldığı açıklanmaktadır. Bunların yanında NSA analisti Edward Snowden'in sızdırmış olduğu bilgilere göre bu casusluk faaliyetleriyle Fransa Dışişleri Bakanlığının verilerinin izlendiği aktarılmıştır. Ayrıca sızdırılan bu bilgilerde, uluslararası para transferinin başrolü SWIFT'in de finansal işlemlerinin izlendiği gibi iddialardan da söz edilmektedir (Prada ve Levine,2013). Globo'nun programı Fantastico'da açıklanan bu rapora göre verilerin doğrudan ABD'li diplomatlar, istihbarat teşkilatları ve Beyaz Saray tarafından sağlandığı açıklanmış; olayın sadece terörle mücadele adına yapılan bir casusluk faaliyeti olmadığı net bir dille aktarılmıştır (Fantastico,2013). Yaşanan olayların ardından Avrupa Parlamentosunda (AP) TFTP'nin askıya alınarak ABD'ye veri akışının kesilmesine dair bir oylama yapılmış, 280 oydan 254'ü veri akışının askıya alınmasına (30 çekimser) onay vermiştir. Fakat AP'de alınan bu kararların bağlayıcılığının olmaması herhangi bir yaptırımı getirmemiştir (European Parliament, 2013).

Kasım 2019'da Avrupa Veri Koruma Denetmeni'nin (EDPS) yayınladığı rapordan aktarıldığına göre Europol'ün TFTP kapsamındaki rolü üzerinde, çerçeve belirleyici bir içerik ortaya çıkmıştır. Ayrıca ABD tarafından, AB topraklarındaki verilerin talep edilmesi durumlarında da sadece terör ve terörizmin finansmanının içeriği ile ilgili veri akışı olacağı bir kez daha net bir dille ifade edilmiştir (LL.M., 2020).

ABD Hazine Bakanlığının açıklamalarına göre son 35 aylık periyotta SWIFT ağından talep edilen verilerin, neredeyse yüzde 40'tan fazlasının Europol ve AB

ülkelerinin talepleri üzerine incelendiği görülmüştür. Ayrıca 2016 ve 2018 arasındaki dönemde TFTP kapsamında ABD, AB ülkeleriyle yaklaşık 80.000 civarı bireysel ipucu paylaştığını aktarmaktadır. Buna 2015 Paris ve 2011 Norveç saldırılarıyla ilgili bazı veriler de dâhildir (Klein, 2020). ABD tarafından kullanılan verilerin oldukça işe yarar olduğu sürekli vurgulanırken, bunların yanında sürekli bu durumdan yakınan AB'nin bir taraftan veri akışında da talepkâr davrandığı görülmektedir.

### 1.4. Öneriler

Görüldüğü üzere bazı çelişkilerin ortaya çıkmasına sebep olan bu düzenleme için çözüm düşünüldüğünde, bunun yine düzenlemeler ve diplomasi aracılığıyla açıklığa kavuşturulması mümkün görünmektedir. Çalışmada elde edilen bilgiler ışığında bazı öneriler aşağıda listelenmiştir.

- Uluslararası para transferlerinin şeffaflaştırılması konusunda, tüm dünya devletlerinin denetim yetkilerini arttıracak bir düzenleme ortaya koyulabilir.
- Finansal veri mesajlaşmaları konusunda yasal düzenlemeler getirerek şirketlerin ve devletlerin tekelleşmelerinin önüne geçilmesi hakkında çalışmalar yürütülmesi ile alternatif kurumların ortaya koyulması üzerine düzenlemeler yapılabilir. (Alternatif yapıların ortaya koyulması, güvenlik ve diğer konularda rekabet oluşturup avantaj sağlayabilecekken, oluşan alternatif yapıların yönetiminde bulunduğu ülkenin çıkarlarını korumaya ve görüşlerini yansıtmaya devam etmesi dezavantaj olabilir.)
- SWIFT'in iki merkezinden birinin ABD'de bulunmasından kaynaklı olarak herhangi bir yasal işlemde, SWIFT ağı ABD yasalarına tabi tutularak hukuki zeminde yargı karşısına çıkmaktadır. Bu sebeple, SWIFT üzerinden terörizmin finansmanı ile ilgili bilgi akışı sağlanırken, ABD ve Belçika dışında geriye kalan ülkelerin hukuki düzenlemelerinden birçok noktada şirket muaf tutulabilir. Buna bir çözüm olarak SWIFT ağını kullanan her ülkede bir ofis açılması ve o ülkenin hukuki zemininde değerlendirilmesine olanak sağlanması üzerine düşünülebilir.
- Bir başka öneri ise her ülkenin SWIFT benzeri bir ağ oluşturmasıdır. Bu noktada SWIFT bir çatı kuruluş olabilir. Bu durumda, her ülkenin kendine ait finansal mesajlaşma ağına sahip olması, o ülkenin hukuki kurallarına tabi olmasını da sağlayacaktır.

Kişisel verilerin korunması ile ilgili çalışmalar oldukça önemlidir; fakat bu durum güvenlik ile ilgili problemleri göz ardı etmeye sebep olmamalıdır. Yapılan çalışmamaların denetimi ve şeffaflaşmasına odaklanılmalı, kişisel verileri korumaya çalışırken güvenlik zafiyetlerinin doğmasının önüne geçilmelidir.

## SONUÇ

Geniş bir araştırma yapıldığında finansal veri mesajlaşma sistemleri konusunda SWIFT ağının dünyada bir tekel hâline geldiğini söylemek ulaşılabilir bir sonuçtur. SWIFT ağı, geçmişten bu yana gerçekten işlemleri hızlandırması ve veri güvenliğini sağlaması ile uluslararası bir itibar kazanmıştır. Bu itibar doğrultusunda güven kazanan şirket; ABD Hazine Bakanlığını, AB ülkelerini haberdar etmeden ve verilerin gizliliğini umursamadan kişisel verilerin korunmasıyla ilgili ihlallerde bulunmuştur. İhlaller sonrası TFTP ile terörizm ve finansmanıyla ilgili konulara özel bir nitelik sağlanmış, bu da bir anlaşma ile güvence altına alınmıştır. Ancak bu güvencelere rağmen bazı ihlallerin daha ortaya çıktığı görülmüştür. Çalışmada bahsi geçen TFTP'nin SWIFT için bağlayıcı olması, kişisel verilerin korunması kapsamında AB yasalarıyla çelişkiler ortaya koymaktadır.

SWIFT'in tam manasıyla güvenilir işlemler yaptığı söylenirken verilerin paylaşılmasıyla birlikte şirket itibarını zedeleyecek gelişmeler yaşanmıştır. Bu durumun sorumlusu direkt olarak SWIFT değildir. Dünyada güvenliğin sağlanması öncelikli bir konudur. Bu yüzden TFTP gibi bir çalışmanın ortaya koyulması bir ihtiyaçtan doğmuştur. TFTP'nin bir ihtiyaç olduğunun bilinmesinin yanında, azami olarak kişisel verilerin korunmasına da dikkat edilebilir. Bu konuda AB kurumları çeşitli çalışmalar yürütmektedir. TFTP'nin kapsamında, SWIFT üzerinden verilerin okunması, gözetlenmesi ve takibi, terörle mücadele etmenin yanında kişisel verilerin gözetlenmesi gibi konular da istismar edilebilmektedir. Ülkelerin kişisel çıkarları, SWIFT verilerinin istismar edilmesine sebep olabilir. Verileri elde etme nüfuzuna sahip ülkenin, ulusal çıkarları doğrultusunda bir terör yapısının finansal kanallarını görmezden gelmesi mümkün gözükmektedir. Dahası elde edilen verilerin çarptırılmasıyla bir ülke ve bireyin itibar suikastına maruz kalması da mümkün olmaktadır.

NSA'nın terörizmin finansmanı dışında, SWIFT verilerini elde ettiğine dair çeşitli bilgiler bulunmaktadır. Elde edilen bilginin ulusal çıkarlar doğrultusunda kullanılmasını engelleyecek hiçbir mekanizma bulunmamaktadır. Bu noktada TFTP, AB ülkelerinin endişe ettiği üzere kişisel verilerin korunması bakımından güvenlik

açıklarıyla dolu gözükmektedir. Bu durumun çözümü için bu çalışmada tekelleşmenin önüne geçilmesi, yasal temsilcilikler ve şeffaflık gibi konularda bazı çözüm önerileri getirilmiştir. TFTP kapsamında SWIFT verilerinin gözetlenmesi günümüzde hâlâ çözüme kavuşmamış bir sorundur.

## KAYNAKÇA

Rusya'nın "alternatif SWIFT" sistemi. (2019). Erişim Tarihi: 21 Nisan 2021, https://www.turkrus.com/791521-rusyanin-alternatif-swift-sistemi-xh.aspx.

Bakirtaş, T. ve Ustaömer, K. (2019). Türkiye'nin Bankacılık Sektöründe Dijitalleşme Olgusu. Ekonomi, İşletme ve Yönetim Dergisi, *3*(1), 1–24. https://doi.org/2602-4195

Barbak, A. (2016, Aralık). Devletlerin Terörizmin Finansmanının Önlenmesi Politikalarının Oluşumu: Küresel Yönetişim ve Mali Eylem Görev Gücü Etkisi". Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Dergisi, 31(2), 147–177.

*Council of European. Processing and protection of personal data subpoenaed by the Treasury Department from the US based operation centre of the Society for Worldwide Interbank Financial Telecommunication (SWIFT)* (No. 11291/2/07 REV 2 (Presse 157)). (2007). Date of Access: 13 May 2021, http://register.consilium.europa.eu/pdf/en/07/st11/st11291-re02.en07.pdf.

Çakır, A. (2006). Bankacılıkta Operasyonel Risklerin Etkin Yönetiminde Risk Bazlı Müşterini Tanı İlkelerinin Önemi. Bankacılar Dergisi, 56, 40–50.

European Parliament. (2013). MEPs call for suspension of EU-US bank data deal in response to NSA snooping. Date of Access: 18 August 2021, https://www.europarl.europa.eu/news/en/press-room/20131021IPR22725/meps-call-for-suspension-of-eu-us-bank-data-deal-in-response-to-nsa-snooping.

Fantastico. (2013). NSA Documents Show United States Spied Brazilian Oil Giant. Date of Access: 12 August 2021, http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html.

Gür, İ. (2009). *Kişisel Verilerin Korunması Hususunda Ab İle Abd Arasında Çıkan Uyuşmazlıklar Ve Çözüm Yolları*.(Yayımlanmamış Yüksek Lisans Tezi). Ankara Üniversitesi, Ankara.

Kedikli, U. (2013). *Uluslararası Terörizm ve Devlet Sorumluluğu*. Ankara: Nobel Akademik Yayıncılık.

Klein, A. (2020). How the US and Europe quietly share data to prevent terrorist attacks. Date of Access: 12 August 2021, https://thehill.com/blogs/congress-blog/homeland-security/531152-how-the-us-and-europe-quietly-share-data-to-

prevent.

Kuzu, Y. (2003). *Türkiye Cumhuriyet Merkez Bankası'nda Uluslararası Elektronik Finansal İletişim ve Yurdışı Ödeme Sistemleri ile İlişkiler*. (Yayımlanmamış Uzmanlık Yeterlilik Tezi). Türkiye Cumhuriyet Merkez Bankası, Ankara.

Lichtblau, E.ve Risen, J. (2006). Bank Data Is Sifted by U.S. in Secret to Block Terror. Date of Access: 28 July 2021, https://www.nytimes.com/2006/06/23/washington/23intel.html.

LL.M., C. R. (2020). Compliance with Terrorist Finance Tracking Programme Agreement. Date of Access: 12 July 2021, https://eucrim.eu/news/compliance-terrorist-finance-tracking-programme-agreement/.

Prada, P. ve Levine, A. (2013). U.S. tapped into networks of Google, Petrobras, others: report. Date of Access: 2 September 2021, https://www.reuters.com/article/us-usa-security-snowden-petrobras-idUSBRE9870AD20130909.

Rapoza, K. (2015). Russia To Retaliate If Bank's Given SWIFT Kick. Date of Access: 8 August 2021, https://www.forbes.com/sites/kenrapoza/2015/01/27/russia-to-retaliate-if-banks-given-swift-kick/?sh=59e91c76652e.

Şahin, B. (2010, Aralık). Karapara ve Karaparanın Aklanmasına İlişkin Ulusal-Uluslar Arası Düzenlemeler. *Trakya Üniversitesi Sosyal Bilimler Dergisi*, 12(2), 152–173.

Servent, A. R. ve Mackenzie, A. (2011, November). Is the EP Still a Data Protection Champion? The Case of SWIFT. Perspectives on European Politics and Society, 12(4), 390–406. https://doi.org/10.1080/15705854.2011.622957

Swift. (2016). SWIFT and the Fight Against Illicit Financial Activity. Date of Access: 12 July 2021, https://www.swift.com/swift-resource/21476/download?language=en.

Swift. (2021a). A secure, global platform for sharing KYC data. Date of Access: 12 July 2021, https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/kyc-registry#:~:text=The KYC Registry is a,data from their correspondent banks.

Swift. (2021b). Monthly FIN traffic evolution. Date of Access: 12 July 2021, https://www.swift.com/about-us/swift-fin-traffic-figures

Talay, I. ve Bayram, O. (2020, Temmuz). Küresel Tedarik Zinciri Ve Uluslararası Ticaret Yönetiminde Verimli Ödeme Sistemi Seçimi. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 34(3), 945–972. https://doi.org/10.16951/atauniiibd.704616.

Terrorist Finance Tracking Program. (2010). Date of Access: 24 August 2021, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/Final Updated TFTP Brochure %288-5-11%29.pdf.

Üstün, O. (2005). Mali Eylem Görev Gücü'nün (FATF) Dokuz Özel Tavsiyesi. *Bankacılar Dergisi*, 52, 10–27. Erişim tarihi: 6 Temmuz 2021, https://www.tbb.org.tr/Dosyalar/Arastirma_ve_Raporlar/FATF_Mart2005.pdf

Üstün, O. (2006). Karapara Aklama ve Terörizmin Finansmanını Önleme Standartlarını Değerlendirme Metodolojisinde Finansal Kuruluşların Yükümlülükleri. *Bankacılar Dergisi,* 56, 51–68. Erişim tarihi: 6 Temmuz 2021, https://www.tbb.org.tr/Dosyalar/Arastirma_ve_Raporlar/karapara_aklama.pdf.

Üstün, O. (2008). Karapara Aklama ve Terörün Finansmanı ile Mücadelede Uluslararası Girişimler ve Araçlara Toplu Bakış. *Bankacılar Dergisi*, 65, 19–36. Erişim tarihi: 7 Temmuz 2021, https://www.tbb.org.tr/Dosyalar/Arastirma_ve_Raporlar/karapara_aklama_ve_terorun_finansmani_ile_mucadele.pdf.

Wakefield, J. (2019). Russia "successfully tests" its unplugged internet.. Date of Access: 2 September 2021, https://www.bbc.com/news/technology-50902496.

Yılmazcan, D. (1998, Ocak). Kara Para Aklama ve Uluslararası Mali Sistem. *Öneri Dergisi*, 2(9), 61–68.